

## Protect Briefing – 14/12/2016



## Tabletop cybersecurity exercises essential to infosec training

Do you have a business continuity plan (BCP) in place in case you are the victim of cybercrime?

A successful BCP should be based on a business impact analysis, with maintaining normal operations as effectively as possible being the ultimate aim.

An important part of any BCP is testing its content. In its simplest form this can be key people sitting around a table pretending to do the things detailed in the plans.

At the extreme full scale simulations can be undertaken.

An article in Techtarget discusses the importance of cybersecurity exercising and how frequently this should take place.

To read the full article visit [Techtarget](#)



**The Cyber Essentials scheme provides business' with clarity on good practice within cyber security.**

**Find out more [here](#).**

## Passwords – will we ever get it right?

Once again the news is full of articles about stolen data and compromised passwords. How safe would you feel if one of your passwords was stolen? How many of your online accounts would be insecure if one of your passwords was in the public arena?

For years the government, law enforcement agencies and private sector companies have warned of the dangers of having simple passwords and using the same password for multiple accounts but we still don't seem to be listening.

A recent [blog](#) by lifebytesweb discusses passwords security and best practice.

## Free DMARC tool released

The [Global Cyber Alliance](#), an international non-profit organization focused on Addressing systemic cyber risks, has announced the release of its first project to fight phishing: a tool to make implementation of DMARC easier.

The tool, available at <https://dmarc.globalcyberalliance.org/> is easy to use and available for anyone to use, free of charge. DMARC (Domain-based Message Authentication Reporting & Compliance) provides brand protection, inbox protection and greater visibility into some of the threats organizations face.

The Global Cyber Alliance (GCA) is an international, cross-sector effort dedicated to confronting cyber risk and improving the connected world. GCA was founded in September 2015 by the Manhattan District Attorney's Office, the City of London Police and the Center for Internet Security.

Learn more at [www.globalcyberalliance.org](http://www.globalcyberalliance.org)



**METROPOLITAN  
POLICE**

**TOTAL POLICING**

NEW  
SCOTLAND  
YARD

## Arrests made in NCA cybercrime investigation

Twelve people have been arrested as part of a National Crime Agency operation targeting users of website crippling software which can cost as little as £4. The investigation centred around the use of Netspoo stresser, a Distributed Denial of Service (DDoS) programme, freely available on the dark web. Operation Vulcanalia was based on intelligence gathered by the West Midlands Regional Cyber Crime Unit and saw more than 60 individuals targeted.

For further information regarding Operation Vulcanalia visit the [NCA website](#)

## Cost of cybercrime has soared to \$280 billion this year

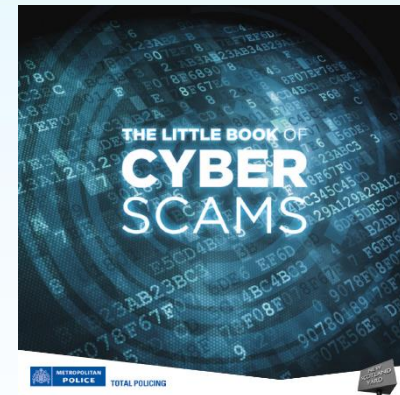
In a new report from Grant Thornton, which involved a survey of 2,500 business in 36 economies worldwide, the firm explores the damages done to companies as well as kinds of attacks currently impacting businesses.

To read more about the survey results visit [consultancy.uk](#)

## Online shopping fraud

As we enter the busy Christmas shopping period it's useful to remember there can be risks associated with shopping online.  
If something seems too much of a bargain it could well be of poor quality, counterfeit or non-existent.  
If making a purchase from an auction or re-sale site, forum or social media site never transfer money directly via bank transfer to people you don't know.  
If you're buying concert or event tickets buy only from official sources and to avoid fraud never pay by direct bank transfer.  
Make sure any new smartphones or devices are protected with a PIN or passcode and have up to date security software installed.

For more information visit [GetSafeOnline](#)



## Briefing Dissemination

This document has been given the protective marking of NOT PROTECTIVELY MARKED and may be disseminated outside of law enforcement with no restrictions. Please feel free to circulate it within your business or to other partners.

If you know anyone else who would like to receive this briefing please send us their e-mail address and we will add them to the distribution list. If you no longer wish to receive this bulletin please let us know at the email address below.

Any comments or queries please email the FALCON Cyber Protect team at:

**CyberProtect@met.police.uk**

